REMARKS

Applicant respectfully requests reconsideration of this application. Claims 1-85 are currently pending. All existing claims have been cancelled. Claims 86-123 have been added.

Therefore, claims 86-123 are now presented for examination.

Revival of Application

A request for non-publication was filed in the present application. While the present application has not been and was not intended to be foreign filed, a continuation-in-part of the present application, U.S. Application Serial No. 10/968,741, was published and foreign filed.

Without any concession regarding any issues, the Applicant hereby petitions for revival and publication of the present application, and provides notice of the foreign filing of U.S. Application Serial No. 10/968,741.

Claim Rejection under 35 U.S.C. §102

Downs, et al.

The Examiner rejected claims 1, 2, 4, 6-8, 10-13, 15, 17, 23-26, 28-36, 38, 39, 41, 43, 44, 46-50, 57, 58, 60, 61, 64-67, 69, 72, 73, 75, 76, and 78-83 under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,574,609 of Downs, et al. (hereinafter referred to as "*Downs*").

All existing claims have been cancelled and replaced with new claims. Claim 86 reads as follows:

86. (New) A method for protecting data in an apparatus having an open system architecture comprising:

receiving encrypted data in the apparatus;

generating raw data in a closed subsystem of the apparatus by decrypting the encrypted data and optionally performing additional processing on the encrypted data;

preventing access to the raw data outside of the closed subsystem;

generating protected data in the closed subsystem by re-encrypting the raw data; and

asserting the protected data from the closed subsystem to an external device or system.

Thus, claim 86 provides for protecting data in an apparatus having an open system architecture, which includes receiving encrypted data, generating raw data in a closed subsystem of the apparatus by decrypting the encrypted data and optionally performing additional processing on the encrypted data, preventing access to the raw data outside of the closed subsystem, and generating protected data in the closed subsystem by re-encrypting the raw data. It is submitted that, among other differences between the claims and the cited reference, *Down* does not include these claim elements. A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631 (Fed. Cir. 1987).

Claim 86 includes processes in a closed subsystem of an apparatus with an open system architecture, which is not addressed by *Downs*. *Downs* generally relates to a secure electronic content management system. However, the secure system operates in a completely different manner and contains different elements than the claim elements. In essence the *Downs* system operates by transferring content to a content host, with metadata and usage condition data being transferred to an electronic store. The content is encrypted with a first encrypting key before being transferred to the content host, and the first encrypting key is encrypted with a second encrypting key. The encrypted first encrypting key is transferred along with the metadata and usage condition data to the electronic store. The metadata and usage condition data are used to form promotional data, and the encrypted first encrypting key is transferred with the promotional data to a customer's system. (See *Downs* abstract and col. 3, lines 48-67) To the degree that the reference regards multiple encryption processes, the reference relates to the encryption of an encryption key. There is no mention of a closed sub-system, system, or other structure.

Within the described system, *Downs* does refer a certain type of "open architecture". However, the term "open" is being used in a completely different sense in *Downs.* Rather than referring to systems configured to allow end users to add or remove hardware components and/or software modules conveniently, as provided in the current application, the reference relates to open systems in the sense that the system is open to different kinds of content and formats:

> The Secure Digital Content Electronic Distribution System (System) is an open architecture with published specifications and interfaces to facilitate broad implementation and acceptance of the System in the market place while maintaining rights protection for the content proprietors. ...
>
> The architecture is open regarding the nature of the Content and its format. Distribution of audio, programs, multimedia, video, or other types of Content is supported by the architecture. ...
>
> The architecture is also open to different distribution networks and distribution models. ...

(*Downs*, col. 8, lines 41-66) Thus, the reference is addressing a different concept using a similar terminology.

With regard to operations within a closed system, the Office Action cites to the following:

> VI. SECURE CONTAINER PACKING AND UNPACKING
>
> A. Overview
>
> The SC(s) Packer is a 32-bit Windows' DLL with an external API (Application Programming Interface) that can be called in either a multiple or single step process to create a SC(s) with all of the specified parts. The SC(s) Packer 151, 152, 153 variety of hardware platforms supporting Windows' DLL at the Content Provider(s) 101, Clearinghouse(s) 105, Electronic Digital Content Store(s) 103 and other sites requiring SC(s) Packing. A BOM and, if necessary, a Key Description part are created and included in the SC(s). A set of packer APIs allows the caller to specify the information required to generate the records in the BOM and Key Description parts and to include parts in the SC(s). Encryption of parts and Symmetric Keys 623 as well as computing the digests and the digital signature is also be performed by the packer. Encryption and digest algorithms that are supported by the packer are included in the packer code or they are called through an external interface.

(*Downs*, col. 37, lines 46-55) This portion of *Downs* relates to "secure container" (also referred to as SC) packing, where a secure container "is a cryptographic carrier of information or content that uses encryption, digital signatures, and digital certificates to provide protection against unauthorized interception or modification of electronic information and content", and which "allows for the verification of the authenticity and integrity of the Digital Content". (*Downs*, col. 7, lines 42-48) In this system, content is encrypted within secure containers and the storage and distribution of the secure containers is separate from control of unlocking and use. (*Downs*, col. 7, lines 52-55) The secure container operates in connection with a clearinghouse, which provides licensing authorization by enabling intermediate or end users to unlock content after verification of a successful completion of a licensing transaction. While the Office Action does not specifically identify the "closed sub-system" of any apparatus or system, but it is submitted that no such closed sub-system is provided here. The "secure container" described in *Downs* is not a sub-system of an apparatus or system, but rather is a data structure that is transmitted. A secure container thus is essentially a particular data element, which might commonly be referred to as a data packet, that includes certain specific elements. For example, Figure 2 illustrates a secure container 200 that includes usage conditions 206, a transaction ID encrypted object 205, an application ID encrypted object 207, and an encrypted symmetric key object 204, which are all signed by an end-user digital signature 202. These are thus simply data elements.

Further, Figure 3 illustrates the encryption process used to generate the secure container data elements. (See *Downs*, col. 15, line 55 to col. 16, line 12) Upon creating the secure container, the secure container is transmitted. "307A Sender must have obtained the certificate from a certification authority prior to initiating secure communications. The certification authority includes in the certificate the sender's public key, the sender's name and signs it. PV CAUTHR refers to the certifications authority's private key. Sender transmits the SC(s) to the recipient." (*Downs*, col. 16, lines 8-12) (emphasis added)

Thus, what *Downs* is discussing is how data structures are generated, including the packing operations discussed in the quoted portion of the reference. No closed sub-system is discussed in this portion of the reference, and Applicant has been unable to locate any such element in the reference.

The Office Action further appears to cite to:

> copied or played; manages the number of copies made (or deletion of the copy) in accordance with the Digital Content's Usage Conditions; and performs the copy to an external media or portable consumer device if permitted. The portable consumer device can perform a subset of the End-User Player Application 195 functions in order to process the content's Usage Conditions embedded in the watermark. The terms End-User(s) and End-User Player Application 195 are used throughout this to mean through the use or running-on an End-User Device(s) 109.
>
> 6. Transmission Infrastructures 107

(*Downs*, col. 12, lines 2-12) The Office Action indicates that "Downs indicates that the content can be re-encrypted by the user player when making a copy". As this portion of the reference does not appear to be connected to the statement in the Office Action, Applicant concludes that there is an error in the Office Action citation. However, Applicant was unable to discern what portion of the reference was intended. Applicant is uncertain what a "user player" indicates in this instance. Downs refers to end-users, and describeds the End-User Player Application 195 which, for example, verifies that an Electronic Digital Content Store 103 is a valid distributor of Content 113. However, this does not seem to relate to the statement in the Office Action. Applicant respectfully requests that the Examiner clarify this portion of the rejection if the rejection is not removed.

The Office Action then cites to:

> C. Overview of Secure Container Flow and Processing

> Metadata SC(s) 620 are built by Content. Provider(s) 101 and are used to define Content 113 items such as songs. The Content 113 itself is not included in these SC(s) because the size of the Content 113 is typically too large for Electronic Digital Content Store(s) 103 and End-User(s) to efficiently download the containers just for the purpose of accessing the descriptive metadata. Instead, the SC(s) includes an external URL (Uniform Resource Locators) to point to the Content 113. The SC(s) also includes metadata that provides descriptive information about the Content 113 and any other associated data, such as for music, the CD cover art and/or digital audio clips in the case of song Content 113.

(*Downs*, col. 25, lines 27-39) Again, this provision indicates that secure containers are data that is to be transferred, with the indication that the size of the content is typically too large for Electronic Digital Content Stores 103 and End-Users to efficiently download the containers just for the purpose of accessing the descriptive metadata. The reference does refer to Electronic Digital Content Stores, which are entities (such as web sites) that market content:

> Electronic Digital Content Store(s) 103 are the entities who market the Content 113 through a wide variety of services or applications, such as Content 113 theme programming or electronic merchandising of Content 113. Electronic Digital Content Store(s) 103 manage the design, development, business operations, settlements, merchandising, marketing, and sales of their services. Example online Electronic Digital Content Store(s) 103 are Web sites that provide electronic downloads of software.

(*Downs*, col. 10, lines 19-27) However, these elements do not appear to relate to the elements of the claims as they do no appear to included closed systems or sub-systems as provided in the claims.

Thus, *Downs* does not contain any teach regarding a system with an open architecture, or a closed sub-system within such a system. *Downs* uses somewhat similar terminology, but the terminology is used in a very different sense and has a very different meaning.

It is thus submitted that claim 86 is not anticipated by *Downs*. It is submitted that the arguments presented above also apply to the independent claims 99, 113, and 119 of the current application and such claims are not anticipated. The remaining claims are dependent claims, and are allowable as being dependent on the allowable base claims.

Claim Rejection under 35 U.S.C. §103

Downs in view of Lee

The Examiner rejected claims 3, 5, 9, 14, 16, 18-22, 27, 37, 40, 42, 45, 51-56, 59, 62, 63, 68, 70, 71, 74, and 77 under 35 U.S.C. 103(a) as being unpatentable over *Downs* in view of U.S. Patent Application Publication 2004/0064694 of Lee, et al. (hereinafter referred to as "*Lee*"). The rejected claims were cancelled.

It is submitted that, in addition to any other differences, *Lee* does not teach or suggest the elements of the claims missing from *Downs*, and thus the references, together or in combination, cannot show the elements of the claims. *Lee* relates to a method and apparatus for augmenting authentication in a cryptographic system. For example, Figure 1 of *Lee* illustrates transmission unit 110 and reception unit 120 containing authentication units 150 and 170, and Figure 2 illustrates a process for augmenting authentication including encryption and transfer of a nonce taken from a communication stream. There does not appear to be any discussion in *Lee* that is relevant to an apparatus with an open system architecture or a closed sub-system of such apparatus.

Claim Rejection under 35 U.S.C. §103

Downs in view of Laksono

The Examiner rejected claims 84 and 85 under 35 U.S.C. 103(a) as being unpatentable over *Downs* in view of U.S. Patent Application Publication 2003/0156218 of Laksono (hereinafter referred to as "*Laksono*"). The rejected claims were cancelled.

It is submitted that, in addition to any other differences, *Laksono* does not teach or suggest the elements of the claims missing from *Downs*, and thus the references, together or in combination, cannot show the elements of the claims. *Laksono* relates to multiplexing channels in a multimedia system. There does not appear to be any discussion in *Laksono* that is relevant to an apparatus with an open system architecture or a closed sub-system of such apparatus.

Conclusion

Applicant respectfully submits that the rejections have been overcome by the amendment and remark, and that the claims as amended are now in condition for allowance. Accordingly, Applicant respectfully requests the rejections be withdrawn and the claims as amended be allowed.

Invitation for a Telephone Interview

The Examiner is requested to call the undersigned at (503) 439-8778 if there remains any issue with allowance of the case.

Request for an Extension of Time

The Applicant respectfully petitions for a three-month extension of time to respond to the outstanding Office Action pursuant to 37 C.F.R. § 1.136(a) should one be necessary. Please charge the necessary fee to our Deposit Account No. 02-2666.

Charge our Deposit Account

Please charge any shortage to our Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: 10/5/2007

/Mark C. Van Ness/
Mark C. Van Ness
Reg. No. 39,865

1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
(503) 439-8778